UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/653,517	08/31/2000	Michael K. MacKay	7451.0029-00	4624

22852 7590 09/06/2007

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
CHEN, SHIN HON	
ART UNIT	PAPER NUMBER
2131	
MAIL DATE	DELIVERY MODE
09/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 09/653,517	**Applicant(s)** MACKAY ET AL.	
	Examiner Shin-Hon Chen	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 August 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 August 2000* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. Claims 1-20 have been examined.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/10/07 has been entered.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-3, 5, 7-9, and 14-20 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Grecsek U.S. Pat. No. 6088801 (hereinafter Grecsek).

5. As per claim 1, Grecsek discloses a method for protecting electronic content from unauthorized use by a user of a computer system, the method including: receiving a request from a user of the computer system of access a piece of electronic media content (Grecsek: column 3

lines 24-33); identifying one or more software modules authorized to execute on the computer system and being responsible for processing the piece of electronic media content and enabling use of the piece of electronic media content by the user (Grecsek: column 3 lines 35-63: identify the process that is associated with the file type being requested); evaluating one or more predefined characteristics of the one or more identified, authorized software modules to determine if the one or more software modules are operable to process the electronic media content in an authorized manner, the evaluating including at least one protection mechanism selected from the group consisting of: evaluating whether the one or more software modules make calls to certain system interfaces; determining whether the one or more software modules include one or more predefined code sequences associated with undesirable behavior; analyzing dynamic timing characteristics of the one of more software modules for anomalous timing characteristics indicative of invalid or malicious activity; determining whether the one or more software modules are included on a list of trusted software modules; determining whether the one or more software modules are included on a list of untrusted software modules; and determining whether the one or more software modules have been digitally signed by a trusted party (Grecsek: column 3 line 64 – column 4 line 6: determine if there is unauthorized command associated with the process); and denying the request to use the piece of electronic media content if the evaluation of one or more predefined characteristics fail to satisfy a set of predefined criteria (Grecsek: column 3 lines 30-33: grant or deny process access).

6. As per claim 2, Grecsek discloses the method as in claim 1. Grecsek further discloses the method including: using the predefined criteria to evaluate the predefined characteristics of the

one or more software modules according to a predefined policy, and basing a decision to deny the request on the outcome of this evaluation (Grecsek: column 3 lines 35-63 and column 4 lines 21-36).

7. As per claim 3, Grecsek discloses a method as in claim 1. Grecsek further discloses evaluating one or more predefined characteristics of the one or more software modules includes computing the cryptographic hash of at least one of the one or more software modules (Grecsek: column 4 lines 50-55).

8. As per claim 5, Grecsek discloses a method for protecting electronic content from unauthorized use, the method including: receiving a request to access a piece of electronic media content (Grecsek: column 3 line 64 – column 4 line 6); generating a first identifier associated with the electronic media content (Grecsek: column 4 lines 7-20); and monitoring at least one system interface for electronic data to be transferred to an output device (Grecsek: column 4 lines 7-27: access request include read, write, and display command); the monitoring including: receiving a piece of electronic data to be transferred to an output device (Grecsek: column 4 lines 7-27 and 50-55); generating a second identifier associated with the piece of electronic data (Grecsek: column 4 lines 7-20; column 4 lines 28-37 and 50-55); comparing the second identifier with the first identifier; taking a predefined defensive action if the second identifier is related to the first identifier in a predefined manner, wherein the predefined defensive action is selected from the group consisting of: modifying at least a portion of the piece of electronic data,

or preventing the transfer of at least a portion of the piece of electronic data to an output device via the system interface (Grecsek: column 4 lines 7-28; column 4 lines 50-55).

9. As per claim 7, Grecsek discloses a method as in claim 5. Grecsek further discloses the first identifier comprises a hash of at least a portion of the electronic content, and in which the second identifier comprises a hash of at least a portion of the piece, of electronic data (Grecsek: column 4 lines 7-20 and 50-55).

10. As per claim 8, Grecsek discloses a method as in claim 5. Grecsek further discloses in which the first identifier comprises a predefined portion of the electronic content and in which the second identifier comprises a predefined portion of the piece of electronic data (Grecsek: column 4 lines 7-20).

11. As per claim 9, Grecsek discloses a method as in claim 5. Grecsek further discloses in which the system interface comprises a file system interface to one or more device drivers (Grecsek: column 3 line 52 – column 4 line 20).

12. As per claim 14, Grecsek discloses a method as in claim 5. Grecsek further discloses in which the predefined defensive action comprises preventing the transfer of at least a portion of the piece of electronic data to an output device via the system interface (Grecsek: column 3 line 64 – column 4 line20).

13. As per claim 15, Grecsek discloses a method as in claim 5. Grecsek further discloses comparing the identifier to determine whether the software is allowed to be executed (Grecsek: column 3 line64 – column 4 line 6).

14. As per claim 16, Grecsek discloses a method as in claim 5. Grecsek further discloses in which the at least one system interface is selected using rules associated with the electronic content, the rules being operable to identify certain system interfaces to which the electronic content is not allowed to be sent (Grecsek: column 3 line 64 – column 4 line20).

15. As per claim 17, Grecsek discloses a method as in claim 9. Grecsek further discloses in which the one or more device drivers are selected from the group consisting of: video display driver, sound driver, SCSI driver, IDE driver, network driver, video capture driver, floppy disk driver, and scanner driver (Grecsek: column 3 line 64 – column 4 line 27).

16. As per claim 18, Grecsek discloses a method as in claim 5. Grecsek further discloses does not explicitly disclose the method comprising: (a)(1) inserting a cryptographic fingerprint into the piece of electronic content, the cryptographic fingerprint containing information relating to the request to access said piece of electronic content (Grecsek: column 4 lines 50-55).

17. As per claim 19, Davis as modified discloses a method as in claim 18, Davis as modified further discloses in which inserting said cryptographic fingerprint into the piece of electronic content includes: (i) authenticating a fingerprinting engine using a cryptographic credential; (ii)

using the fingerprinting engine to insert the cryptographic fingerprint into the piece of electronic content (Grecsek: column 4 lines 50-55).

18. As per claim 20, Grecsek discloses a method as in claim 19. Grecsek further discloses in which the fingerprinting engine is operable to authenticate a calling application using a cryptographic credential (Grecsek: column 4 lines 50-55).

Claim Rejections - 35 USC § 103

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

20. Claims 4, 6, and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grecsek in view of Davis U.S. Pat. No. 6064739 (hereinafter Davis).

21. As per claim 4, Grecsek discloses a system for protecting electronic content, the system comprising: means for evaluating one or more predefined characteristics of the drivers responsible for handling the electronic content, the means for evaluating including means for operating a protection mechanism selected from the group consisting of: means for evaluating whether the one or more software modules make calls to certain system interfaces; means for determining whether the one or more software modules include one or more predefined code sequences associated with undesirable behavior; means for analyzing dynamic timing

characteristics of the one of more software modules for anomalous timing characteristics indicative of invalid or malicious activity; means for determining whether the one or more software modules are included on a list of trusted software modules; means for determining whether the one or more software modules are included on a list of untrusted software modules; and means for determining whether the one or more software modules have been digitally signed by a trusted party (Grecsek: column 3 lines 24-63); means for denying effective access to the electronic content based on an output of said means for evaluating one or more predefined characteristics of the drivers responsible for handling the electronic content (Grecsek: column 3 lines 30-33: grant or deny process access); means for generating an identifier associated with the electronic content (Grecsek: column 3 line 64 – column 4 line 6); means for monitoring a predefined system interface for data to be transferred to an output device and containing the identifier (Grecsek: column 3 lines 35-50; column 4 lines 21-27: resource access includes read, write, and display); means for preventing effective access to data containing the identifier via the predefined system interface (Grecsek: column 3 lines 24-35). Grecsek does not explicitly disclose applying a cryptographic fingerprint to the electronic content. However, Davis discloses encrypting content to be protected before authorized access (Davis: abstract). It would have been obvious to one having ordinary skill in the art to apply cryptographic fingerprint to the electronic content stored within the computer system because multiple data protection schemes can be applied to a protected data. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Davis within the system of Grecsek because it increases data protection by applying cryptographic fingerprint on the data itself.

22. As per claim 6, Grecsek discloses the method as in claim 5. Grecsek does not explicitly disclose the method including: (a)(1) decrypting the electronic content (Davis: column 2 lines 16-29). However, Davis discloses decrypting content to be protected after authorized access (Davis: abstract). It would have been obvious to one having ordinary skill in the art to apply cryptographic fingerprint to the electronic content stored within the computer system because multiple data protection schemes can be applied to a protected data. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Davis within the system of Grecsek because it increases data protection by applying cryptographic fingerprint on the data itself.

23. As per claim 10, Grecsek discloses a method as in claim 5. Grecsek does not explicitly discloses re-encrypting/modifying the piece of electronic data when the data is stored in the buffer to prevent software probing. However, Davis discloses that limitation (Davis: column 2 lines 16-29 and column 1 lines 50 – column 2 line 29 and column 7 lines 6-28). It would have been obvious to one having ordinary skill in the art to re-encrypt the data when it is transferred between devices. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Davis within the system of Grecsek because it prevents protected data being intercepted in plaintext form.

24. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Grecsek in view of Davis and further in view of Ciacelli et al. U.S. Pat. No. 6236727 (hereinafter Ciacelli).

25. As per claim 11, Grecsek as modified discloses a method as in claim 10. Grecsek as modified does not explicitly disclose in which modifying at least a portion of the piece of electronic data includes scrambling at least a portion of the piece of electronic data. However, Ciacelli discloses scrambling portion of electronic data to protect copyright data (Ciacelli: column 2 lines 3-65). It would have been obvious to one having ordinary skill in the art at the time of invention to combine the teachings of Ciacelli within the system of Grecsek because scrambling a digital data protects the data from being viewed or used by unauthorized parties.

26. Claims 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grecsek in view of Shimada European Patent No. EP0915620 (hereinafter Shimada).

27. As per claim 12 and 13, Grecsek discloses a method as in claim 5. Grecsek does not explicitly disclose the predefined defensive action comprises adding noise/electronic watermark to at least a portion of the piece of electronic data. However, Shimada discloses that limitation (Shimada: [0011]-[0017]). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Shimada within the system of Grecsek because burying noise and digital watermark into data prevents unauthorized copy of a recorded data by an recording/reproducing device.

Response to Arguments

28. Applicant's arguments filed on 8/10/07 have been fully considered but they are not persuasive.

Regarding applicant's remarks, applicant argues that the prior art of record does not disclose identify one or more software modules authorized to execute on the computer system. However, the examiner disagrees. According to Grecsek, Grecsek discloses identifying authorized software modules to execute on the computer system (Grecsek: column 3 lines 52-63: Process I may be identified by a specific file type… a file type can be associated with a process that automatically services it). Therefore, Grecsek discloses identifying authorized process that can execute on the computer system and then capability assessor determines whether the process can execute in authorized manner (Grecsek: column 3 line 64 – column 4 line 6).

On the other hand, applicant argues that the prior art does not disclose means for monitoring a predefined system interface for data to be transferred to an output device. However, Grecsek discloses that the policy assessor determines whether request to access (e.g. Read, write, or display) is to be granted (Grecsek: column 4 lines 21-27: read, write, and display require data to be transferred to an output device). Therefore, applicant's argument is traversed.

Conclusion

29. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

SDMI, "SDMI Portable Device Specification Part 1 Version 1.0 " discloses checking whether a device or application is SDMI compliant before execution of the device/application based on information contained in the digital data indicating whether the data should be protected.

Benson et al. U.S. Pat. No. 5845281 discloses controlling usage of digital data after it has been transmitted to intended users and checking the data to see if there is any control data in embedded in the data intended to restrict the use of the digital data.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon Chen
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

SC